

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/088896 A1

(51) International Patent Classification⁷: **H04L 9/08**, 29/06

(21) International Application Number:

PCT/IB2005/050834

(22) International Filing Date: 7 March 2005 (07.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04100997.8 11 March 2004 (11.03.2004) EP

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **POPESCU, Bogdan, C.** [RO/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **KAMPERMAN, Franciscus, L., A., J.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

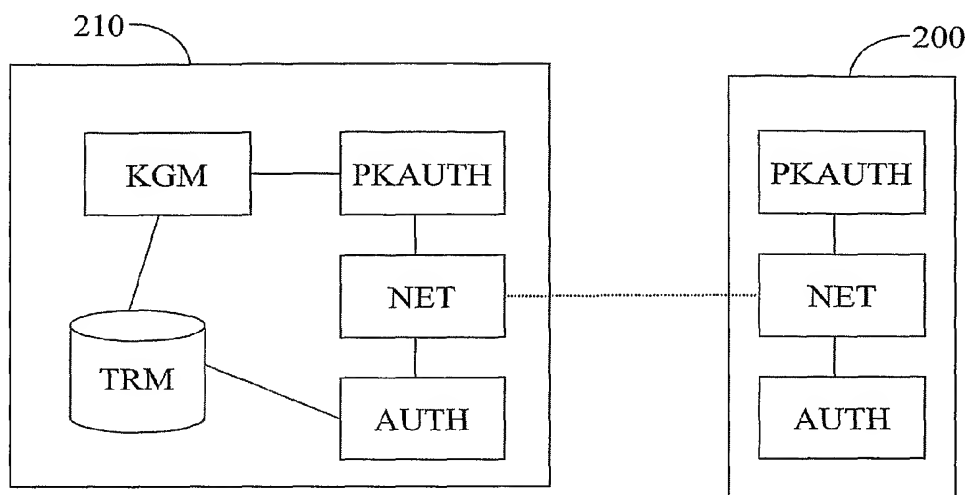
(74) Agents: **GROENENDAAL, Antonius, W., M.** et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: IMPROVED DOMAIN MANAGER AND DOMAIN DEVICE



(57) Abstract: A domain manager device for managing a network. The manager issues to a new device joining the network a number of symmetric authentication keys, and preferably a number of authentication tickets. Each respective authentication key allows the new device to communicate securely with one respective other device comprised in the network. Each respective authentication ticket allows a device with a first identifier to authenticate itself to a device with a second identifier. The new device receives those authentication tickets whose first identifier matches its identifier. The new device presents the ticket with second identifier 'B' to device 'B' to authenticate itself to 'B'. Preferably the domain manager generates a number of master device keys and issues one to the new device. Then the authentication tickets can be encrypted with the master device key issued to device with the second identifier.

WO 2005/088896 A1



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.